UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/746,305	12/21/2000	Kevin L. Wiley	062891.0424 (IOS 2392)	1828

7590 05/04/2005

Terry J. Stalford
Baker Botts L.L.P.
2001 Ross Avenue
Dallas, TX 75201-2980

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/746,305	WILEY ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 January 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-46 and 50-56* is/are allowed.

6)☒ Claim(s) *21-38,47-49 and 54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *see attached*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed with respect to the rejection of independent claims 1,21, and 39 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn.

2. Applicant's arguments filed with respect to independent claim 47 have been fully considered but they are not persuasive.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a key combination being a subset of, and less granular than a root keyset) are not recited in the rejected independent claim 47. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 21-38,47-49, and 54 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Independent claims 21 and 54 recite of "logic encoded in media" and referencing the applicant's specification, it is disclosed on page 9, lines 2-9, that the media can be

"transmission media" which is non-statutory and the claims currently recite of software alone, and of itself. It is suggested by the examiner that the claims be amended so that the media is something tangibly embodying, such as a hardware device such as a computer disk or be amended to show that the logic is processed or executed.

As per independent claim 47, the claims recite of software alone, and of itself. The claim currently recite of just software which is not tangibly embodied and the examiner suggests amending the claims to recite that they are stored on computer readable medium or the data is executed by a processor.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 47-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S. Patent 5,850,516 in view of Conklin et al, U.S. Patent 5,991,881.

As per claim 47, Schneier discloses of data tree structures (datasets) for an intrusion detection system (col. 5, lines 65-67). A plurality of pointers identify child datasets having combinations derived from, and less granular than the root (col. 6, lines 25-66). The teachings of Schneier are silent in disclosing of a keysets that are included in the datasets that are representative of a network connection. The examiner notes that a keyset is broadly interpreted as being data indicative of attack profiles as is

recited in the applicant's specification on page 3, lines 6-7 and page 10, lines 17-21. It is disclosed by Conklin et al of network data is sent in the form of packets which include various identification information (keysets) that is used to transmit data for establishing and maintaining connections (col. 2, line 64 through col. 3, line 14). Conklin et al discloses of keysets comprising a source address and a destination address key (col. 3, lines 3-11 and col. 4, lines 61-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply means of maintaining keyset data that indicates certain characteristics of network activity. Conklin et al recites motivation for the use of keysets by disclosing that these keysets, or descriptions, provide useful information when it comes to detection an intrusion since some of this information can become predictable (col. 4, line 61 through col. 5, line 9). It is obvious that since the teachings of Schneier are dedicated towards detecting attacks, the teachings would have been improved by tracking additional identification information, or keysets, that describes the patterns of attacks as is disclosed by Conklin et al.

As per claim 48, Conklin et al teaches of a termination status indicator (col. 4, line 61 through col. 5, line 9). Please refer above for the motivational benefits of applying Conklin et al to the teachings of Schneier.

As per claim 49, it is disclosed by Schneier that a pointer identifies a sibling root dataset of the root dataset (col. 6, lines 25-66 and as shown in Figure 3).

Allowable Subject Matter

7. Claims 1-46 and 50-56 are allowed over the prior art of record.

The examiner notes that claims 21-38 and 54 are currently rejected under 35 USC 101 for claim non-statutory subject matter.

8. The following is a statement of reasons for the indication of allowable subject matter:

As per claims 1,21, and 39, it was not found to be taught in the prior art of storing data representative of network activity in datasets, the datasets include root datasets each having a root keyset and child datasets each having a child keyset with a key combination being a subset of, and less granular than a root keyset.

As per claims 52 and 55, it was not found to be taught in the prior art of receiving a traffic signature not having a root dataset, generating a root dataset having a root keyset representative of the traffic signature, identifying all existing child and sibling root datasets of the root dataset, generating absent child and sibling root datasets of the root dataset, and associating the child and sibling root datasets of the root dataset.

As per claims 53,54, and 56, it was not found to be taught in the prior art of identifying a child dataset of a root dataset through the root dataset, retrieving data for processing a traffic signature by searching a data storage system including the datasets for an existing root dataset having a root keyset corresponding to the traffic signature and identifying all child datasets, sibling root datasets, and child datasets of the sibling root datasets through the root dataset wherein the data representative of network activity is stored in datasets that include root datasets having a root keyset and child

datasets having child keysets with a key combination derived from and less granular than a root dataset.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

5/2/05

CR
May 2, 2005